IN THE CLAIMS:

The following is a current listing of claims and will replace all prior versions and listings of claims in the application. Please amend the claims as follows:

1-133. (Canceled)

134. (Currently Amended) A tangible computer-readable memory medium storing program instructions within a security program that are executable on an information handling system to:

receive data from an external network coupled to the information handling system, wherein the received data includes a first set of data for a web page;

analyze the first set of data to make a determination whether the first set of data indicates that it is from a first source coupled to the external network, ~~; and~~ wherein the determination is based, at least in part, on an age of the first set of data;

upon the determination that the first set of data is actually from the second source, provide output from the information handling system indicative of the determination.

135. (Previously Presented) The tangible computer-readable memory medium of claim 134, wherein the first set of data includes information indicating that it is from a source trusted by a user of the information handling system.

136. (Previously Presented) The tangible computer-readable memory medium of claim 135, wherein the first set of data is intended to cause the user to supply confidential information to a source other than the trusted source.

137. (Previously Presented) The tangible computer-readable memory medium of claim 136, wherein the confidential information is financial information of the user.

138. (Previously Presented) The tangible computer-readable memory medium of claim 136, wherein the confidential information is login information of the user.

139. (Currently Amended) A method, comprising:

~~receiving a web page at~~ a security program on a first computing device receiving a web page via a wide-area network, wherein the web page includes information indicating that its origin is a first source that is trusted by a user of the first computing device;

the security program on the first computing device sending data that is requested by the web page to the origin of the web page; ~~and~~

the security program on the first computing device analyzing the origin's response to the sent data to make a determination[[e]] whether the origin of the web page is the first source; and

upon the determination that the origin of the web page is not the first source, providing output from the first computing device that is indicative of the determination.

140-141. (Canceled)

142. (Previously Presented) The method of claim 139, wherein the web page solicits confidential information from the user.

143-152. (Canceled)

153. (Currently Amended) A method, comprising:

a security program on a computing device making a determination of the likelihood that a web page received via ~~from~~ a ~~first~~ computer network is misrepresented as being from a trusted source, including:

the security program analyzing a layout of the received web page; ~~and~~

the security program determining that the layout of the received web page is similar to a layout of a known mistrusted web page;

upon determining that the layout of the received web page is similar to the layout of the known mistrusted web page, the computing device providing output indicative of the likelihood that the received web page is misrepresented as being from the trusted source.

154. (Currently Amended) The method of claim 153, wherein said making said determination further includes the security program determining whether the web page's markup language contains the trusted source's name or logo and whether the web page has the same organization of content as the trusted source.

155. (Currently Amended) A method, comprising:

a security program on a computing device making a determination of the likelihood that a web page received via ~~from~~ a ~~first~~ computer network is misrepresented as being from a trusted source, wherein the determination is based on one or more of the following criteria: an age of the web page, a size of the web page, a number of hyperlinks to the web page from trusted sources; and

the computing device providing output indicative of the determination.

156. (Previously Presented) The method of claim 155, wherein the determination is based, at least in part, on the age of the web page and the size of the web page.

157. (Previously Presented) The method of claim 155, wherein the determination is based, at least in part, on the age of the web page and the number of hyperlinks to the web page from trusted sources.

158. (Currently Amended) A tangible computer-readable memory medium storing program instructions within a security program that are executable on a computing device to:

make a determination of the likelihood that a web page received via ~~from~~ a ~~first~~ computer network is misrepresented as being from a trusted source coupled to the ~~first~~ computer network, including:

analyzing a layout of the received web page; ~~and~~

determining that the layout of the received web page is similar to a layout of a known mistrusted web page;

upon determining that the layout of the received web page is similar to the layout of the known mistrusted web page, provide output from the computing device indicative of the likelihood that the received web page is misrepresented as being from the trusted source.

159. (Currently Amended) A tangible computer-readable memory medium storing program instructions within a security program that are executable on a computing device to:

make a determination of the likelihood that a web page received at the computing device from a ~~first~~ computer network is misrepresented as being from a trusted source, wherein the determination is based on one or more of the following criteria: an age of the web page, a size of the web page, a number of hyperlinks to the web page from known trusted sources; and

provide output from the computing device indicative of the determination.

160. (Currently Amended) A tangible computer-readable memory medium storing program instructions within a security program that are executable on a computing device to:

receive a web page ~~at a first computing device~~ via a wide-area network, wherein the web page includes information indicating that its origin is a first source that is trusted by a user of the ~~first~~ computing device;

send data that is requested by the web page to the origin of the web page; ~~and~~

analyze the origin's response to the sent data to make a determination[[e]] whether the origin of the web page is the first source; and

upon the determination that the origin of the web page is not the first source, provide output from the computing device indicative of the determination.

161. (Currently Amended) A tangible computer-readable memory medium storing program instructions within a security program that are executable on an information handling system to:

receive data from an external network coupled to the information handling system;

analyze the received data to make a determination whether the received data indicates that it is from a first source coupled to the external network, but is actually from a second source coupled to the external network, ~~; and~~ wherein the determination is based, at least in part, on a size of the received data;

upon the determination that the received data is actually from the second source, provide output from the information handling system indicative of the determination.

162. (Previously Presented) The tangible computer-readable memory medium of claim 161, wherein the received data is data for a first web page, and wherein the determination is based, at least in part, on the size of the first web page.

163. (New) The tangible computer-readable memory medium of claim 134, further comprising program instructions within the security program that are executable on the information handling system to block display of the web page by the information handling system upon the determination that the first set of data is actually from the second source.

164. (New) The tangible computer-readable memory medium of claim 134, wherein the output from the information handling system is provided by the security program to a user of the information handling system that requested the web page.

165. (New) The tangible computer-readable memory medium of claim 134, wherein the output from the information handling system is provided by the security program via a network to a security provider.

166. (New) The method of claim 139, further comprising the security program blocking display of the web page by the first computing device upon the determination that the origin of the web page is not the first source.

167. (New) The method of claim 139, wherein the output is provided to a user of the first computing device that requested the web page.

168. (New) The method of claim 139, wherein the output is provided via a network to a security provider.

169. (New) The method of claim 153, further comprising the security program blocking display of the web page by the computing device upon determining that the layout of the received web page is similar to the layout of the known mistrusted web page.

170. (New) The method of claim 153, wherein the output is provided to a user of the computing device that requested the web page.

171. (New) The method of claim 153, wherein the output is provided via a network to a security provider.

172. (New) The method of claim 155, further comprising the security program blocking display of the web page by the computing device upon determining that the web page is likely misrepresented as being from the trusted source.

173. (New) The method of claim 155, wherein the output is provided to a user of the computing device that requested the web page.

174. (New) The method of claim 155, wherein the output is provided via a network to a security provider.

175. (New) The tangible computer-readable memory medium of claim 158, further comprising program instructions within the security program that are executable on the computing device to block display of the web page by the computing device upon determining that the layout of the received web page is similar to the layout of a known mistrusted web page.

176. (New) The tangible computer-readable memory medium of claim 158, wherein the output from the computing device is provided by the security program to a user of the computing device that requested the web page.

177. (New) The tangible computer-readable memory medium of claim 158, wherein the output from the computing device is provided by the security program via a network to a security provider.

178. (New) The tangible computer-readable memory medium of claim 159, further comprising program instructions within the security program that are executable on the computing device to block display of the web page by computing device upon determining that the web page is likely misrepresented as being from the trusted source.

179. (New) The tangible computer-readable memory medium of claim 159, wherein the output from the computing device is provided by the security program to a user of the computing device that requested the web page.

180. (New) The tangible computer-readable memory medium of claim 159, wherein the output from the computing device is provided by the security program via a network to a security provider.

181. (New) The tangible computer-readable memory medium of claim 160, further comprising program instructions within the security program that are executable on the computing device to block display of the web page by the computing device upon the determination that the origin of the web page is not the first source.

182. (New) The tangible computer-readable memory medium of claim 160, wherein the output from the computing device is provided by the security program to a user of the computing device that requested the web page.

183. (New) The tangible computer-readable memory medium of claim 160, wherein the output from the computing device is provided by the security program via a network to a security provider.

184. (New) The tangible computer-readable memory medium of claim 161, further comprising program instructions within the security program that are executable on the information handling system to block display of the received data by the information handling system upon the determination that the received data is actually from the second source.

185. (New) The tangible computer-readable memory medium of claim 161, wherein the output from the information handling system is provided by the security program to a user of the information handling system that requested the received data.

186. (New) The tangible computer-readable memory medium of claim 161, wherein the output from the information handling system is provided by the security program via a network to a security provider.